

رجال الرئيس؟

داخل إدارة البحوث التقنية، اللاعب السري في البنية التحتية للاستخبارات في مصر



تود منظمة الخصوصية الدولية Privacy International أن تشكر أفرادا لا يمكن تسميتهم، على مساعدتهم لإتمام هذا التحقيق. خاطر بعض هؤلاء مخاطرة كبيرة لإشراكنا في المعلومات التي يمتلكونها، الأمر الذي نقدره كثيرا.
هذا التقرير مبني أساسا على وثائق أصلية أعطيت في ثقة و سرية إلى منظمة الخصوصية الدولية. تقريرنا مبني أيضا على معلومات صارت متاحة علنا عن مبيعات و أنشطة شركات التنصت، كما أجرينا لإتمامه مقابلات مع دارسين بارزين لوكالات الاستخبارات المصرية.
منظمة الخصوصية الدولية هي الجهة الوحيدة المسؤولة عن هذا التقرير.
اتصلنا أثناء إعداد هذا التقرير بالشركات التالية: التقنية الألمانية الحديثة Advanced German Technology ، وإيه.سكس للاستشارات A6 Consultancy ، ومجموعة جي.إن.إس.إي GNSE Group ، وهاكِنج تِيم Hacking Team ، ومجموعة نوكيا Nokia Group ، وسيمنس Siemens ، وسولف آي.تي Solve IT ، والأنظمة الكونية المتقدمة Universal Advanced Systems . و بالإضافة، فقد اتصلنا بالحكومة المصرية. كما أن محاولاتنا للاتصالبالمصرية الألمانية لصناعات الاتصالات Egyptian German Telecommunication Industries لم تكن ناجحة.

مقدمة

لوكالات الاستخبارات اليوم دور مركزي في أمن أي حكومة. و عندما لا تقع تحت الرقابة، يصير دورها أكثر غموضا، و تنمو إمكاناتها كثيرا، و تتوسع أغراضها لما يتعدى أمن الناس. و في البلاد غير الديمقراطية، سرعان ما يصبح أمن الحكومة هو أولويتها الأولى.
ترتبط قصة وكالات الاستخبارات المصرية بتاريخ مصر من الحكم الاستبدادي. و كلما ظهرت معلومات عن الوكالات الاستخباراتية المصرية، نجد بعض مكونات مجتمع الاستخبارات المصري لم يصبه أي قدر من التدقيق حتى ذلك الحين. يلقي هذا التقرير لمنظمة الخصوصية الدولية الضوء على وجود إدارة البحوث التقنيةTechnical Research Department، و هي وحدة سرية مكانها غالبا داخل المخابرات العامة المصرية. دخلت إدارة البحوث التقنية في دائرة اهتمامنا بسبب طموحها الكبير لشراء معدات التنصت. نكشف في هذا التقرير عددا من شركات التنصت الأوروبية التي ما برحت تتعامل مع إدارة البحوث التقنية، و هي إدارة ظَل دورها قابعا في الظلام عبر تاريخ البلاد من الحكم الاستبدادي و ثورتها مؤخرا.
يظهر تقرير منظمة الخصوصية الدولية إدارة البحوث التقنية باعتبارها لاعبا سريا أساسيا في عالم الاستخبارات المصري، و يوثق للإمكانات التي حصلت عليها الإدارة من شركات غربية—متضمنة شبكات نوكيا سيمنس و هاكِنج تِيم—اللتان باعتها الإدارة تقنيات تنصت متطورة، حتى عندما كانت مصر، و هي لا تزال، في مخاض مواجهات عنيفة.

أجهزة الاستخبارات المصرية

تتشكل وكالات الاستخبارات المصرية من المخابرات العامة، و إدارة المخابرات الحربية و الاستطلاع، و جعاز مباحث الأمن الوطني، و هيئة الرقابة الإدارية.
أثر ثاني رؤساء مصر جمال عبد الناصر كثيرا في البنية التحتية الحالية للاستخبارات. فقد خطط بعد انقلاب1952 كي تلعب مصر دورا قائدا في حركة عدم الانحياز الصاعدة بين الدول الأفريقية و الآسيوية. و لذلك الغرض، فقد قرر أنه من المطلوب

تأسيس خدمة تسهل هذه الأجندة من خلال العمليات السرية، و بأن تصبح بمثابة أعين مصر و آذانها. كانت المخابرات العسكرية في ذلك الوقت تركز على إسرائيل باعتبارها الخطر العسكري الرئيسي. و كان ذلك هو الوقت الذي أسست فيه المخابرات العامة كي تنفذ تلك المهمة الجديدة، و هي القيام بعمليات سرية ذات طابع غير عسكري.
أكثر أجهزة الاستخبارات المصرية ظهورا عالميا هو جهاز مباحث الأمن الوطني، و هو وحدة الاستخبارات داخل وزارة الداخلية، و الذي زعم تفكيكه في العام2011 بعيد انتفاضة الربيع العربي التي أنهت حكم الرئيس حسني مبارك. اعتبر جهاز مباحث الأمن الوطني مسؤولا عن الكثير من القمع و انتهاكات حقوق الإنسان تحت حكم مبارك.[1] إن حل واحد من وكالات الاستخبارات هو عمل نادر، و عادة ما يكون دالا على احتياج كبير للتغيير، إلا أن جهاز مباحث الأمن الوطني ما لبث أن أعيد ضباطه إلى الخدمة في2013 أثناء الحكومة المؤقتة للرئيس عدلي منصور بعد الإطاحة بالإخوان المسملين، و قبل أن تتولى حكومة السيسي البلاد.[2]

أما المخابرات العامة فهي وكالة الاستخبارات الرئيسية المنوط بها جمع الاستخبارات محليا و خارج البلاد، و مقرها الرئيسي في ضاحية كوبري القبة في القاهرة. لا تتبع المخابرات العامة أي وزارة في الحكومة و تقع مباشرة تحت مسائلة رئيس الجمهورية[3] الذي يعين رئيس المخابرات العامة.[4]
بينما تُحَدَّدُ لوكالات الاستخبارات السابق ذكرها مهمات واضحة و رؤساء معروفين، تعمل إدارة البحوث التقنية في سرية تامة— لدرجة أن وجودها لم تعترف به الحكومة المصرية في أي وقت.

إلقاء الضوء على الظلال: سياق عمل إدارة البحوث التقنية

تاريخ من القمع السياسي

بالرغم من أن تاريخ إنشاءها غير واضح، و من مقابلات مع أحد دارسي الاستخبارات، فإن إدارة البحوث التقنية أنشئت أثناء حكم الرئيس حسني مبارك باعتبارها وحدة داخل المخابرات العامة تخضع لمسائلته مباشرة. ترأس مبارك نظام حكم بالغ الفساد في الفترة بين1981 و2011.

طبقا لما هو متاح، أنشأ مبارك هذه الوحدة ليضمن أن حكومته قادرة على السيطرة على المعارضة السياسية، و يبدو أنها أنشئت كوحدة تتمتع بالاستقلال الكامل داخل المخابرات العامة—وحدة يستطيع الرئيس الاستعانة بها، فرضا، عندما ترفض المخابرات القيام بأنشطة معينة.

إلا أنه من غير الواضح بالضبط التاريخ الذي أنشئت فيه إدارة البحوث التقنية. تقترح التواريخ في بعض الوثائق التي اطلعنا عليها أن إدارة البحوث التقنية كانت منشأة بالفعل أثناء رئاسة أنور السادات، سلف مبارك.

1 “Egypt dissolves notorious internal security agency”, BBC, 15 March 2011, http://www.bbc.co.uk/news/world-middle-east-12751234

2 “Egypt restores feared secret police units”, The Guardian, 29 July 2013, http://www.theguardian.com/world/2013/jul/29/egypt-restores-secret-police-units

3 “General Intelligence Service (GIS) Mukhabarat”, GlobalSecurity.org, http://www.globalsecurity.org/intell/world/egypt/gis.htm

4 “El-Sisi visits General Intelligence Service headquarters”, Ahram Online, 1 January 2015, http://english.ahram.org.eg/NewsContent/1/64/119293/Egypt/Politics-/ElSisi-visits-General-Intelligence-Service-headqua.aspx

إلا أنه بالرغم من هذا الغموض، فإنه من الواضح أن إدارة البحوث التقنية تعكس نزعة تاريخية في مصر أن يقبض فيها رأس الدولة على الأمور بقبضة من حديد، حتى فيما يتعلق بكبار أعضاء حكومته. فبعد توليه الرئاسة، سجن السادات اثنين من أقوى الأعضاء في الحكومة السابقة: وزير الداخلية شعراوي جمعة، و هو المسؤول عن البوليس السري؛ و نائب الرئيس علي صبري.

في فبراير2011، خضعت حكومة الرئيس حسني مبارك لضغوط المظاهرات التي اجتاحت المنطقة بأسرها، إلا أن إدارة البحوث التقنية لم تتأثر بذلك. ففي ذات العام، اشترت إدارة البحوث التقنية مركزا للمراقبة و نظاما لإدارة اعتراض الاتصالات، و هي بنى تحتية مهمة لاعتراض الاتصالات في الشبكات.

حكم المجلس الأعلى للقوات المسلحة البلاد مؤقتا بعد سقوط مبارك و حتى يونيو2012، حين وصل للرئاسة حزب العدالة و الحرية الذي شكلته جماعة الإخوان المسلمين، و ذلك بعد انتخابات ديمقراطية أجريت ذلك الشهر. و في نوفمبر2012، علق الرئيس محمد مرسي الدستور. و بعد أقل من سنة، في يوليو2013، أطاح الجيش بقيادة الفريق أول عبد الفتاح السيسي الحكومة الجديدة في انقلاب عسكري.[5]

ما لبثت الحكومة الجديدة و حظرت جماعة الإخوان المسلمين باعتبارها "منظمة إرهابية"، كما منع أعضاؤها من المنافسة في الانتخابات مستقبلا.[6] عين السيسي أولا عدلي منصور، و هو وقتها رئيس المحكمة الدستورية العليا، رئيسا مؤقتا للجمهورية. و في يونيو 2014 ، تولى السيسي الحكم بعد انتخابات رئاسية حصل فيها على96% من الأصوات.[7]

طبقا لمنظمات حقوقية، خضعت جماعة الإخوان المسلمين للكثير من القمع هي و أفراد يزعم انتمائهم إليها منذ وصول حكومة السيسي للسلطة، فقد وصفت هيومان رايتس ووتش مقتلة رابعة—التي قتل فيها على الأقل1,150 متظاهرا في أغسطس 2014--"جريمة ضد الإنسانية".[8]

القمع يستمر بلا هوادة. فقد تعرضت المنظمات غير الحكومية و النشطاء في مصر للمزيد من الحملات. يمنع قانون الحق في الاجتماعات العامة و المواكب و التظاهرات السلمية رقم107 لسنة2013 المظاهرات في مصر. استخدم هذا القانون، الذي لقي انتقادا شديدا في المراجعة الدورية الشاملة في الأمم المتحدة في نوفمبر2014[9]، لتبرير القبض على كثير من معارض الحكومة و نشطاء المجتمع المدني. في ديسمبر2014، أصدر رئيس الجمهورية قرارا بقانون يعاقب من يتلقى تمويلا أجنبيا "بقصد ارتكاب عمل ضار بمصلحة قومية" بعقوبة تصل للسجن المؤبد.[10] كان هذا القرار ضربة رئيسية وجهت للمجتمع المدني المصري و للمنظمات الإعلامية، التي يعتمد كثير منها على التمويل الأجنبي.[11]

و بالإضافة، فقد كان الصحافيون أيضا أحد ضحايا هذه الهجمة على الحقوق المدنية الأساسية.

---

5 "Egypt: Abdul Fattah al-Sisi profile", BBC, 16 May 2014, http://www.bbc.co.uk/news/world-middle-east-19256730

6 "Egypt's Muslim Brotherhood faces election ban", Al Jazeera, 15 April 2014, http://www.aljazeera.com/news/middleeast/2014/04/egypt-muslim-brotherhood-faces-election-ban-2014415155426994730.html

7 "Abdel Fatah al-Sisi won 96.1% of vote in Egypt presidential election, say officials", The Guardian, 3 June 2014, http://www.theguardian.com/world/2014/jun/03/abdel-fatah-al-sisi-presidential-election-vote-egypt

8 "Egypt: Rab'a Killings Likely Crimes Against Humanity", Human Rights Watch, 12 August 2014, https://www.hrw.org/news/2014/08/12/egypt-raba-killings-likely-crimes-against-humanity

9 "Egypt - 20th Session of Universal Periodic Review", UN Web TV, 5 November 2014, http://webtv.un.org/meetings-events/human-rights-council/universal-periodic-review/20th-upr/watch/egypt-20th-session-of-universal-periodic-review/3876287212001

10 "Egypt's human rights group 'targeted' by crackdown on foreign funding", The Guardian, 24 September 2014, http://www.theguardian.com/world/2014/sep/24/egypt-human-rights-crackdown-foreign-funding

11 *Ibid*

ففي العام2013، قبض على ثلاثة صحافيين يعملون لدى قناة الجزيرة الدولية—و هم الأسترالي الجنسية بيتر جريسته، و المصري الكندي محمد فهمي فاضل، و المصري الجنسية باهر محمد—و حكم عليهم بالسجن سبع سنوات (عشرة في حالة السيد باهر محمد) بتهم التآمر مع الإخوان المسلمين لنشر أخبار كاذبة.[12]

كما قبض على ثلاثين صحفيا في العام2014[13] و قتلت الصحفية ميادة أشرف بالرصاص أثناء مسيرة. صرح زميل لميادة أشرف شهد الهجوم أنها ضربت بالرصاص أثناء هروبها من إطلاق نار قادم من ناحية الشرطة، بينما أنكرت الشرطة الاتهامات.[14]

في نوفمبر2015، ألقى الجيش القبض على حسام بهجت، مؤسس المبادرة المصرية للحقوق الشخصية، و هي إحدى المنظمات الحقوقية المصرية، و الصحافي في مدى مصر، لأسباب تتعلق بمقالات كتبها عن الجيش، و جرى احتجازه ثلاثة أيام.[15]

يأتي تأسيس و وجود وحدة استخبارات سرية كإدارة البحوث التقنية متسقا مع نمط أوسع من القمع السياسي من طرف جهات أمنية لا تخضع للمحاسبة، كما أنه يتعارض مع بلد يفترض أنها تمر بتحول ديمقراطي.

مكتب داخل المخابرات العامة

يقع مقر إدارة البحوث التقنية في ضاحية كوبري القبة في القاهرة، و ذلك طبقا لوثائق من شركة تقنيات التنصت التقنيات الألمانية الحديثة و شركة هاكِنج تِيم (طالع الملحقات). كوبري القبة هو أيضا الحي الذي يقع فيه مقر المخابرات العامة. في رسالة بريد إلكتروني مسربة من شركة التنصت هاكِنج تِيم، كتب أحد موظفي الشركة أن مقر إدارة البحوث التقنية يقع في نفس المبنى الذي يحوي "الخدمة السرية"، دون أن يحدد أي الخدمات السرية يعني.[16] يأتي هذا متسقا مع المعلومات التي قدمها أحد دارسي الاستخبارات الذي تحدثنا معه، و الذي أكد أن إدارة البحوث التقنية هي وحدة داخل المخابرات العامة. من الجدير بالذكر أيضا أن في عديد الوثائق التي سربت على مدار السنوات الخمس الماضية من شركات التنصت، لم يظهر اسم المخابرات العامة أبدا. يدل هذا أيضا على أن إدارة البحوث التقنية ما برحت تشتري تقنيات التنصت لحساب المخابرات العامة.

الجوع لمزيد من التقنيات

تمتلك إدارة البحوث التقنية إمكانات تنصت واسعة النطاق، كما يوضح نطاق تقنيات التنصت التي اشترتها. يشمل هذا مركزا لمراقبة الاتصالات، و نظاما لإدارة اعتراض الاتصالات، و برمجيات تجسس شديدة الاقتحام.

يظل غير واضحا ما إذا كانت موازنة إدارة البحوث التقنية منفصلة عن موازنة المخابرات العامة، و إذا ما كانت التقنيات التي تشتريها إدارة البحوث التقنية تستخدمها أيضا المخابرات العامة. يبدو أن إدارة البحوث التقنية تمتع بموازنة كبيرة الحجم، فقد

---

12 "Egypt Deports Peter Greste, Journalist Jailed with 2 Al Jazeera Colleagues", The New York Times, 1 February 2015, http://www.nytimes.com/2015/02/02/world/africa/egypt-releases-and-deportsal-jazeera-journalist-from-australia.html

13 "2015 World Press Freedom Index – Egypt", Reporters Without Borders, 2015, https://index.rsf.org/#!/index-details/EGY

14 "Mayada Ashraf", Committee to Protect Journalists, 2014, https://cpj.org/killed/2014/mayada-ashraf.php

15 "A statement by Hossam Bahgat on his military detention, interrogation.", Mada Masr, 10 November 2015, http://www.madamasr.com/sections/politics/statement-hossam-bahgat-his-military-detention-interrogation

16 لا يبدو أن موظفي هاكينج تيم زاروا مقر إدارة البحوث التقنية، حيث جرت المقابلة في مكاتب الوسيط، و لم يكن لهم إلا اتصال محدود بموظفي إدارة البحوث التقنية. ويكيليس هاكِنج تِيم، رسالة بريد إلكتروني رقم14661

https://wikileaks.org/hackingteam/emails/emailid/14661

توقعت هاكِنج تِيم أن تحصل على مليون يورو من بيع تقنيات تنصت اقتحامية لها، و ذلك طبقا لدراسة عملاء هاكِنج تِيم المسربة، و هي وثيقة إدارية تسرد المبالغ التي يدفعها كل عميل من عملاء الشركة سنويا.

و طبقا لمصدر في صناعة التنصت على علم بها، تتطلع إدارة البحوث التقنية دائما إلى تقنيات جديدة، فقد أخبرنا هذا المصدر أنه "إذا بدأت شركة تبيع نوعا من التقنيات تهتم به [إدارة البحوث التقنية]، فلن تحتاج أن تسعى وراءهم. هم سيتحرون عنك و يتصلون بك عاجلا أم آجلا."

موازنة رئاسية

تتمتع إدارة البحوث التقنية، مثلها مثل المخابرات العامة، بموازنة مستقلة عن وزارة الدفاع و وزارة الداخلية، و التي تدير كل منهما وحدة استخبارات خاصة بها. في رسائل بريد إلكتروني عن صفقات محتملة مع إدارة البحوث التقنية، وضح موظفي هاكِنج تِيم أن إدارة البحوث التقنية لا يحاسبها إلا رئيس الجمهورية، و هو أيضا من يخصص لها موازنة مباشرة.[17] و بالرغم من أن موازنتها غير معلنة، فإنها، طبقا لأحد المصادر، "أكبر موازنات وكالات الاستخبارات فيما يتعلق بحلول النظم الأمنية."

"إن غرض زيارتنا هو مقابلة إدارة البحوث التقنية في المخابرات لعرض إثبات نظري**proof of concept**. التقينا بهم ليوم و نصف، و مر كل شيء بسلاسة [...]. في اليوم الثاني، ظهر رئيس الإدارة لبضع ساعات. و كانوا كلهم سعداء جدا و قرروا شراء نظام التحكم عن بعد**Remote Control System** (نحن نتحدث عن أكثر من مليون يورو).

---بريد إلكتروني من**m******a@hackingteam.it** إلى **rs****s@hackingteam.it** يوم**21** يونيو **2013**."

استخبارات سرية جدا

بينما يعرف الجمهور بوجود المخابرات العامة و إدارة المخابرات الحربية و الاستطلاع، كما يعرفون رؤسائها، لا تظهر إدارة البحوث التقنية في الوثائق الرسمية إلا تلميحا. قد يكون سبب هذا هو سرية مهمتها، و التي تبدو، طبقا لمصدر استخباراتي على دراية بإدارة البحوث التقنية، أنها وكالة استخبارات شخصية لرئيس الجمهورية. يظهر أن غرض الإدارة جزئيا هو أن تتجسس على باقي موظفي الحكومة و على الخصوم المحتملين. لا يؤسس أي نص قانوني أو قرار لوجود إدارة البحوث التقنية.

و بالرغم من ذلك، فإن إدارة البحوث التقنية كيان حقيقي، فهي عميل لمصر للأنظمة الهندسية **Systems Engineering Egypt** ، و الأخيرة هذه شركة تبيع منتجات وكالة عن مصنعي تقنيات التنصت مثل بلو كوت**Blue Coat** (و التي تطور تقنيات الفحص العميق للرزم**deep packet inspection**) وأكسس **Axis** (التي تصنع معدات و برمجيات الدوائر التليفزيونية المغلقة).[18]

17 ويكيليكس هاكِنج تِيم رسالة بريد إلكتروني رقم**14661**
https://wikileaks.org/hackingteam/emails/emailid/14661

18 عملاء مصر للنظم الهندسية
http://www.seegypt.com/selected%20customers.asp

من يدير إدارة البحوث التقنية؟

يظهر من سير موظفين سابقين في إدارة البحوث التقنية أنها تعين أفرادا حاصلين على إجازات الدكتوراة في الإلكترونيات و الهندسة أو في الحوسبة. أشار أحد موظفي هاكِنج تِيم إلى مديرة إدارة البحوث التقنية، التي ادعى أنه قابلها، باللواء ليلى.[19] و هو أمر لافت للنظر باعتبار أن أغلبية جيش مصر من الذكور. يشار إلى المديرة في وثائق أخرى بالدكتورة ليلى، ما يلمح إلى أنها تحوز أيضا على إجازة الدكتوراة. غير أن واحدة من الفواتير المرسلة إلى إدارة البحوث التقنية موجهة إلى "عزيزي السيد" (طالع الملحقات). يقترح أفراد على دراية بهيكل الاستخبارات المصرية أن ترأس امرأة إدارة البحوث التقنية ليس بالضرورة أمرا مثيرا للدهشة. فالإدارة يبدو أنها تعين أكاديميين بالأساس، ما لا يجعل وجود امرأة خبيرة بالهندسة، على سبيل المثال، أمرا غريبا. و طبقا لما أوضح المصدر العليم بالمؤسسات المصرية، إذا كان جزءا من مهام مدير إدارة البحوث التقنية أن يرأس ضباطا عسكريين، فمن المعقول أن تمنح رتبة "اللواء" الفخرية، و هو إجراء معتاد للمدنيين الذين يجدون أنفسهم يقودون أفرادا عسكريين.

إمكانات التنصت الواسع لإدارة البحوث التقنية

شبكات نوكيا سيمنس: تمنح إدارة البحوث التقنية أعينا و آذانا

كانت شبكات نوكيا سيمنس شراكة بين تكتل الأعمال الألماني سيمنس آ.جيه و شركة الاتصالات الفنلندية نوكيا. باعت شبكات نوكيا سيمنس أحد أجزاءها، و هو "سيمنس للحلول الاستخباراتية**Siemens Intelligence Solutions**" إلى محفظة شركاء بيروسا**Perusa Partners Fund 1 LP**، و هي مؤسسة استثمار خاصة مقرها ميونخ. أطلق على الشركة الجديدة تروفيكور **Trovicor**[20] ، و ذلك بعد جدل دار في2009 عندما اكتشف أن شبكات نوكيا سيمنس باعت معدات مركز للمراقبة في إيران.[21]

إلا أن شبكات نوكيا سيمنس و تروفيكور استمرتا في العمل سويا تحت مسميات "مورد شبكات نوكيا سيمنس**NSN Vendor**" و "طرف ثالث سيورد الخدمات في البلاد نيابة عن شبكات نوكيا سيمنس".[22]

توضح وثائق غير منشورة حصلت عليها منظمة الخصوصية الدولية عن أعمال شبكات نوكيا سيمنس في مصر، أنه في العام**2011** باعت شبكات نوكيا سيمنس شبكة إكس 25 إلى إدارة البحوث التقنية—و هي تقنية عتيقة تسمح بالوصول إلى إنترنت بطريق الاتصال الهاتفي. تسمح هذه التقنية بالوصول إلى إنترنت حتى لو أغلقت البنية التحتية الرئيسية لإنترنت في البلاد، كما حدث في مصر أثناء الثورة.

---

19 ويكيليكس هاكِنج تِيم رسالة بريد إلكتروني رقم14661 https://wikileaks.org/hackingteam/emails/emailid/14661

20 "Trovicor", Perusa, 24 April 2009, http://www.perusa-partners.de/deutsch/beteiligungen/liste/trovicor.php and "Provision of Lawful Intercept capability in Iran", Nokia, 22 June 2009, http://networks.nokia.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran

21 "Iran's Web Spying Aided By Western Technology", The Wall Street Journal, 22 June 2009, http://online.wsj.com/ news/articles/SB124562668777335653?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB124562668777335653.html

22 "Tipping the scales: Security and surveillance in Pakistan", Privacy International 21 July 2015, https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

كما باعت شبكات نوكيا سيمنس إلى إدارة البحوث التقنية، إما في2011 أو قبلها،نظام إدارة اعتراض الاتصالات ، ومركز مراقبة شبكات الهواتف الثابتة و المحمولة. تتيح هاتان التقنيتان إمكانات للتنصت الواسع، ما يمكن الحكومة المصرية من اعتراض الاتصالات الهاتفية لأي خط يمر عبر نظام إدارة اعتراض الاتصالات.

تُظهر الوثائق أيضا أن شركة الأنظمة الكونية المتقدمة، و هي شركة تقدم نفسها باعتبارها "مزود حلول رائد للأنظمة المشروعة لاعتراض الاتصالات في مصر"[23]، قد توسطت في بيع هذه المنتجات. تزعم شركة الأنظمة الكونية المتقدمة أنها "الوكيل الحصري لأكثر من عشرة شركات دولية (أوروبية و أمريكية)." لا تظهر شبكات نوكيا سيمنس أو تروفيكور رسميا كشركاء لها.

شركة أخرى كانت طرفا في تعاملات شبكة إكس 25 هي المصرية الألمانية لصناعات الاتصالات، المملوكة جزئيا لشركة سيمنس و الموصوفة بأنها "شراكة بين الحكومة المصرية و سيمنس آ.جيه ألمانيا."[24] على المستوى الوطني، فالمصرية الألمانية لصناعات الاتصالات هي أيضا الشركة المسؤولة في مصر عن تركيب مقاسم (سنترالات) إي.دبليو.إس.دي، و هي أنظمة مقاسم للهواتف الأرضة و المحمولة.[25]

اعتراض الاتصالات لغرض مشروع

تقنيات اعتراض الاتصالات هي أدوات تتطلب تركيبها داخل الشبكة كي تتنصت على الاتصالات، و هي على النقيض من تقنيات تكتيكية كأدوات التنصت المحمولة و التي لا تتطلب تركيبها داخل الشبكة كي تعمل. تتلقى هذه التقنيات التكتيكية البيانات لاسلكيا أو مباشرة من الأجهزة التي تراقبها. عادة ما يجمع تركيب تقنيات اعتراض الاتصالات ثلاثة أنواع من الشركاء التجاريين، يقدم كل منها منتجا أو خدمة:

- النوع الأول من هؤلاء الشركاء التجاريين هومُصَنّعُ المعدات التي تشكل أساس الشبكة، و المصنع في هذه الحالة هو شبكات نوكيا سيمنس. تتضمن المعدات التي تبيعها هذه الشركات المبدلات**switches** و المقاسم**exchanges** التي تستخدم في تمرير الاتصالات بين الخطوط، بالإضافة إلى عتاد آخر و خدمات تضمن أن البنية التحتية للاتصالات ككل قادرة على دعم مختلف أنواع الشبكات و الخدمات.
- النوع الثاني من أولئك الشركاء التجاريين هو مزود خدمة الاتصالات**telecommunications service provider**، الذي يدير الشبكة و يحصل أموالا من العملاء لقاء الخدمات. يضمن مزودي الخدمة أن أنشطتهم تتوافق مع التشريعات الوطنية للبلاد التي يعملون فيها، و هو أمر يتضمن عادة اشتراطا قانونيا يتطلب من مزودي خدمات الاتصالات تيسير وصول إدارات إنفاذ القانون و الوكالات الأمنية المختلفة إلى شبكاتها و إلى بيانات مشتركيها.
- النوع الثالث من الشركاء التجاريين هوشركة تقنيات التنصت **surveillance technology company**—مثل شركة الأنظمة الكونية المتقدمة—التي تُسَوِّق مباشرة و تبيع المنتجات و الخدمات لأغراض الاستخبارات و إنفاذ القانون. توفر هذه الشركات "حلولا" مصممة لتمكين الإدارات الحكومية من اعتراض بيانات الاتصالات و تحليلها و

23 About UAS
http://www.uas-eg.com/about.html

24 EGTI The High Technology Company, Internet Archive, 4 December 2000,
https://web.archive.org/web/20001204204500
http://egti.com/profile.htm

25 *Ibid*

توزيعها. تبيع شركات تقنيات التنصت حلولها إما مباشرة إلى الحكومات أو إلى مزودي خدمات الاتصالات.

توجد اشتراطات قانونية في كثير من البلاد تلزم مزودي خدمات الاتصالات بجعل شبكاتها متوافقة مع متطلبات اعتراض الاتصالات. لذا يفضل بعض مزودو خدمات الاتصالات التعامل مع شركات التنصت على حسابها، و تضمين حلول التنصت الإلكتروني في شبكاتها. تتطلب الحكومات حول العالم أن يجعل مقدمو خدمات الاتصالات شبكاتهم متطابقة مع معايير "الاعتراض المشروع للاتصالات **Lawful Interception**." يشكل معيار قانون مساعدة الاتصالات لإنفاذ القانون **Communications Assistance for Law Enforcement Act** في الولايات المتحدة، و معيار معهد معايير الاتصالات الأوروبية **European Telecommunications Standards Institute** في أوروبا مثالين لتلك الأطر المصممة كي تضمن أن كل شبكات الاتصالات و مصنعي معداتها و مقدمي خدمات الاتصالات يصممون البنية التحتية للاتصالات بشكل يسمح للدول الوصول إليها.

تنص المادة 64 من قانون تنظيم الاتصالات لسنة 2003 في مصر على أنه

> ومع مراعاة حرمة الحياة الخاصة للمواطنين التى يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات والتى تتيح للقوات المسلحة وأجهزة الأمن القومى ممارسة اختصاصها فى حدود القانون.

لا يحدد القانون على سبيل الحصر "أجهزة الأمن القومي" التي يحق لها اعتراض الاتصالات، لذا فإن اعتراض إدارة البحوث التقنية للاتصالات في الأغلب قانوني باعتبار ذلك التعريف القانوني الغامض.[26]

إن شراء إدارة البحوث التقنية لتقنيات التنصت الواسع كمراكز المراقبة و أنظمة إدارة اعتراض الاتصالات هو أمر مقلق للغاية، فمبيعات شركة تروفيكور من تلك التقنيات إلى البحرين و إيران تسببت في موجات غضب عالمية. استخدمت سلطات الحكومة البحرينية هذه التقنيات للقبض على خصوم لها ثم عذبتهم بعد ذلك بينما قُرِئَت عليهم محتوى رسائلهم النصية و محادثاتهم الهاتفية.[27] و في إيران، زُعِمَ استخدام مراكز المراقبة التي باعتها شبكات نوكيا سيمنس خلال اضرابات مظاهرات 2009 بغرض قمع النشطاء.[28]

باعتبار سجل مصر في حقوق الإنسان، فمن المثير للقلق البالغ أن تحوز وحدة سرية كإدارة البحوث التقنية، و التي لا يظهر وجود أي نوع من الرقابة عليها أو المهام المحددة قانونا لها، إمكانات تنصت تمكنها من مراقبة الاتصالات الهاتفية و على إنترنت لكل من هم في مصر. لدى مصر بالفعل تراث من استخدام التنصت كوسيلة لنشر الخوف. فبعد مظاهرات 2011، بث برنامج تليفزيوني محادثات هاتفية بين نشطاء معروفين ليقلل من مكانتهم في أعين الجمهور.[29] قالت ناشطة مصرية أن محتوى رسائل بريدها الإلكتروني و دردشاتها على إنترنت مع شريكها مررت تحت عقب بابها، و ذلك قبل استدعائها من قبل جهاز مباحث الأمن الوطني (أمن الدولة) للاستجواب بفترة قصيرة.[30]

---

26 المادة 64 من قانون تنظيم الاتصالات رقم 10 لسنة 2003
http://www.tra.gov.eg/uploads/law/law_en.pdf

27 **"Torture in Bahrain Becomes Routine With Help From Nokia Siemens", Bloomberg, 22 August 2011, http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking**

28 **"Iran's Web Spying Aided By Western Technologies", Wall Street Journal, 22 June 2009, http://www.wsj.com/articles/SB124562668777335653#mod=rss_whats_news_us**

29 **"Egyptians fear return of surveillance state", Al Monitor, 15 January 2014, http://www.al-monitor.com/pulse/originals/2014/01/egypt-eavesdropping-scandal-fear-return-police-state.html#**

30 **"Sexual assault and the state: A history of violence", Mada Masr, 7 July 2014, http://www.madamasr.com/sections/politics/sexual-assault-and-state-history-violence**

التقنيات الألمانية الحديثة: عقد ألماني آخر لإدارة البحوث التقنية

طبقا لوثيقة اخرى حصلت عليها منظمة الخصوصية الدولية ننشرها في الملحقات، اشترت إدارة البحوث التقنية كذلك تقنيات من شركة التقنيات الألمانية الحديثة في2006. الشركة التي تعيد بيع أنظمة التقنيات الألمانية الحديثة في مصر ذلك الوقت كانت شركة مصر للنظم الهندسية.[31] تخصص شركة التقنيات الألمانية الحديثة في الاعتراض المشروع للاتصالات و تفتخر بأنها باعت تقنيات لجهات حكومية عديدة بما فيها جهات استخباراتية. و من غير الواضح نوع التقنيات التي بيعت و إذا ما كانت تقنيات للتنصت. تشير الوثائق إلى تلك التقنيات بمسميات إس.جي.إس-1100 **SGS-1100 1100** و إس.جي-1100 **SG-1100 1100**، و هي تكلف**21,188** و**18,688** دولارا أمريكا على الترتيب. و في الإجمالي، أنفقت إدارة البحوث التقنية ما يزيد على**50,000** دولارا أمريكا على منتجات اشترتها من شركة التقنيات الألمانية الحديثة، شاملة "الدعم الأساسي".

هاكِنج تِيم و فِن فِشر: أدوات إدارة البحوث التقنية للاستهداف

عميل هاكِنج تِيم الغامض

في العام2015، اختُرِقت شركة هاكِنج تِيم: أكثر من مليون رسالة بريد إلكتروني و عديد الوثائق الإدارية المخزنة على خواديمها صارت متاحة للعامة. كُشِف، مرة بعد المرة، تورط الشركة في بيع أنظمة تجسس شديدة الاقتحام إلى حكومات قمعية. تُنتج هاكِنج تِيم برمجية خبيثة تدعى ريموت كونترول سيستم**Remote Control System** تسمح للمهاجم بالتحكم الكامل في حاسوب المستهدَف. يستطيع المهاجم عندها، مثلا، أن يصل إلى أي محتوى مخزن على الحاسوب، و أن يراقب استخدامه أولا بأول، و أن يسجل كبسات المفاتيح و كلمات المرور، و أن يأخذ صورا لما هو معروض على الشاشة و أن يشغل كاميرا الحاسوب.

استخدم ريموت كنترول سيستم للتجسس على الصحافيين و النشطاء. ففي العام2014، أظهر باحثون في مركز سِتِزِن لاب **Citizen Lab**، التابع لجامعة تورنتو، استخدام ريموت كنترول سيستم ضد مجموعة من الصحافيين الإثيوبيين.[32] كما استهدف صحافيون و ناشطون في المغرب و الإمارات، ما أثر بشكل جدي على عملهم و على سلامتهم العقلية.[33]

كانت إدارة البحوث التقنية واحدا من عملاء هاكِنج تِيم الكبار، و كانت على استعداد أن تدفع مليون يورو ثمنا لترخيص استخدام البرمجية و لخدمة العملاء.[34]

ظهر في التسريبات عقدين لإدارة البحوث التقنية: الأول كان مبدئيا مع وسيط يعرف باسم إيه.سكس للاستشارات و بعدها مع سولف آي.تي. أما العقد الثاني فكان مع مجموعة جي.إن.إس.إي، و هي شركة تابعة لمجموعة منصور للأعمال، و التي تمتلكها ثاني أغنى العائلات في مصر. تقدم جي.إن.إس.إي نفسها باعتبارها شركة توفر خدمات "تأمين المعلومات، و التطبيقات

31**http://www.seegypt.com**

32 “Hacking Team and the Targeting of Ethiopian Journalists”, Citizen Lab, 12 February 2014, **https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/**

33 تقرير منظمة الخصوصية الدولية***Their Eyes on Me*, highlights the experiences of individuals targeted using RCS in Morocco** **https://privacyinternational.org/?q=node/554**

34 ويكيليكس هاكِنج تِيم رسالة بريد إلكتروني رقم**602607** **https://wikileaks.org/hackingteam/emails/emailid/602607**

و الشبكات.[35]

يبدو أن العقد مع إيه.سكس لم يكن قد انقضى بحلول يونيو2015 . ففي وثيقة استعراض عملاء2015، لا يزال اسم إيه.سكس يظهر تحت العملاء المحتملين و يُتوقع أن تدفع750,000 يورو ذلك العام.

تظهر رسالة بريد إلكتروني من مارس2015[36] نوع القدرات التي تحاول إدارة البحوث التقنية الحصول عليها:

"ستقود إدارة البحوث التقنية المفاوضات مع هاكِنج تِيم. تطلب إدارة البحوث التقنية عرضا لثلاثة أنظمة مختلفة، كل منها مجهز ب 200 رخصة (و نفس الإعدادات). تود إدارة البحوث التقنية أن تحصل على خصم كمية لشراء ثلاثة أنظمة في وقت واحد، و أن يكون لكل نظام: نفس الإعدادات كما نوقشت سابقا (شاملا ذلك البرمجيات و200 رخصة + العتاد + الخدمات + التدريب في الموقع و في مقر هاكِنج تِيم). ضمان لسنتين شاملا تحديث البرمجيات بسعر نهائي800 ألف يورو لكل نظام (3 × 800,000 = 2,400,000 يورو). يمكن إتمام الصفقة إما بعقد واحد أو بالعقود الثلاثة في وقت واحد. إذا ما قبلت هاكِنج تِيم بالشروط أعلاه، يمكن إتمام الصفقة في غضون شهر واحد."

كان عقد مجموعة جي.إن.إس.إي قد انقضى عندما سربت المراسلات. أظهرت وثيقة استعراض العملاء أن المجموعة مدينة لهاكِنج تِيم بمبلغ412,000 يورو في2105 و أن15,000 يورو كانت قد دُفعت.

بهذا الإجمالي، كما يظهر في قائمة العملاء المسربة، تستطيع إدارة البحوث التقنية استهداف25 جهازا، و هي كمية متوسطة بالمقارنة ببلاد أخرى مثل تايلاند و المكسيك و أوزبكستان.

كانت لإدارة البحوث التقنية طلبات مخصوصة من هاكِنج تِيم. أظهرت المراسلات مع جي.إن.إس.إي أن إدارة البحوث التقنية أرادت استهداف هواتف آيفون و حواسيب ماك من إنتاج آبل. إلا أن الإدارة كانت تخطط أيضا لاستهداف مستخدمي وندوز—فقد شرحوا لهاكِنج تِيم أن من بين مستخدمي وندوز اللذين يرغبون في استهدافهم، يستخدم90% منهم نسخا غير قانونية من نظام التشغيل[37] لذا فقد رغبت الإدارة أن تصمم هاكِنج تِيم البرمجية الخبيثة بحيث لا تستهدف فقط منتجات آبل، و لكن أيضا النسخ غير القانونية من مايكروسوفت وندوز.

فِن فِشر: التقاط الأهداف بطعم "سري و خاص"

طبقا لدراسة نشرها سِتِزِن لاب في أكتوبر2015، استخدمت إدارة البحوث التقنية أيضا فِن فِشر، و هي مجموعة برمجيات خبيثة اقتحامية أخرى مماثلة لمنتجات هاكِنج تِيم.[38]

تمكن سِتِزِن لاب من التعرف على عشرين اسم نطاق ذوي صلة بإدارة البحوث التقنية. استخدم خادوم فِن فِشر عناوين بروتوكول إنترنت مطابقة لتلك التي استخدمها موظف هاكِنج تِيم يوم كان قد رتب موعدا لتركيب نسخة من نظام هاكِنج تِيم

35 عن جي.إن.إس.إي
http://www.gnsegroup.com/Profile/aboutGNS.aspx

36 ويكيليكس هاكِنج تِيم رسالة بريد إلكتروني رقم554233 تمت مطالعتها بتاريخ03/08/2015

37 و يكيليكس هاكِنج تِيم رسالة بريد إلكتروني رقمID 602607 تمت مطالعتها بتاريخ03/08/2015
https://wikileaks.org/hackingteam/emails/emailid/602607

38 "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation", Citizen Lab, 15 October 2015, https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

لدى إدارة البحوث التقنية. وجد الباحثون عينة فن فلايFinFly على إحدى صفحات الوب—و هي صفحة أنشئت لإصابة الأهداف بعدوى برمجيات فِن فِشِر الخبيثة.[39] تعرف الباحثون أيضا على عنوان بروتوكول إنترنت استخدمه خادوم فِن فِشِر و استطاعوا ربطه بعنوان بروتوكول إنترنت آخر مملوك لإدارة البحوث التقنية.[40]

طبقا لسِتِزِن لاب، استخدمت مجموعة مول راتسMOLERATS، و هي مجموعة إجرامية رقمية استهدفت مجموعات "الإسلام السياسي" و إسرائيل، برمجيات خبيثة يبدو أنها مرتبطة بإدارة البحوث التقنية، ما يقترح علاقة بين جهاز المخابرات و المجموعة. استخدمت مول راتس لالتقاط أهدافها طُعما عبارة عن ملف يَعِدُ باحتواءه صور طيار حربي أردني حُرق حيا.[41]

و في ملاحظة أخرى لسِتِزِن لاب، خُبئت برمجية فِن فِشِر داخل وثيقة عنوانها "تقرير سري للغاية". مرة ثانية، كانت البرمجية تتصل بعنوان بروتوكول إنترنت تم التعرف عليه باعتباره من عناوين إدارة البحوث التقنية.[42]

كتابة الفصل التالي

سعى هذا التقرير أن يظهر وجود إدارة البحوث التقنية، و هي وحدة بالغة السرية يرجح أن تكون جزءا من المخابرات العامة. لا تخضع إدارة البحوث التقنية إلا لمساءلة رئيس الجمهورية و يبدو أن مهمتها تتضمن جمع الاستخبارات عن أفراد آخرين داخل أفرع الحكومة المختلفة و سلطاتها. أظهرنا بعض تقنيات التنصت التي اشترتها الوحدة: فمن ناحية، اشترت معدات للتنصت الواسع على الاتصالات، و من ناحية أخرى اشترت برمجيات خبيثة للتجسس بالاستهداف. و بينما لا نزعم أن إدارة البحوث التقنية تقوم نفسها بالتنصت الواسع، إلا أنها تمتلك حاليا على الأقل جزءا من المعدات اللازمة للتنصت الواسع، دون أن تخضع لأي آلية للرقابة أو قبل نقاش برلماني.

تظل أسئلة كثيرة عن إدارة البحوث التقنية بلا إجابات. متى أنشئت على وجه الدقة؟ لماذا أنشئت؟ ما مهمتها؟ إلى أي مدى تتعاون مع أجهزة الاستخبارات الرئيسية في البلاد؟ هل استخدمت المخابرات العامة التقنيات التي اشترتها إدارة البحوث التقنية؟ من يرأس إدارة البحوث التقنية فعلا؟ من يراقب أداءها؟

الشفافية في الاستخبارات أمر ضروري في المجتمعات الديمقراطية. إن وجود وحدة سرية – غير معروفة للجمهور العام و يبدو أنها تعمل دون أي رقابة ديمقراطية – قادرة على إنفاق ملايين اليورو لغرض قد يكون التنصت على اتصالات كل مواطن مصري هو مشكلة حقوق إنسان خطيرة ينبغي على الحكومة المصرية أن تواجهها. نأمل أن يشكل هذا التقرير حافزا لمزيد من البحث و الاستقصاء.

في يوليو2014، دعى البرلمان الأوروبي لحظر تصدير تقنيات المراقبة لمصر. هذه خطوة أولى في الاتجاه الصحيح.

تطلب منظمة الخصوصية الدولية من الحكومة المصرية أن تعلن بوضوح وجود إدارة البحوث التقنية و أن تعلن دورها. ينبغي أن يُشرَح للجمهور ماهية عملياتها و أن تخضع للرقابة. ينبغي أن يوضع إجراء للإذن القضائي لطلبات التنصت التي تقوم بها إدارة البحوث التقنية، و ينبغي أن تتوافق الوحدة مع القانون الدولي. مصر من الدول الموقعة على الإعلان العالمي لحقوق الإنسان و على العهد الدولي للحقوق المدنية و السياسية، و كلاهما يحمي بوضوح الحق في الخصوصية.

تحث منظمة الخصوصية الدولية مصر على أن تكون أكثر شفافية بكثير فيما يتعلق ببنيتها التحتية التي تتيح التنصت، و أن تضمن أنها متوافقة تماما مع القانون الدولي.

---

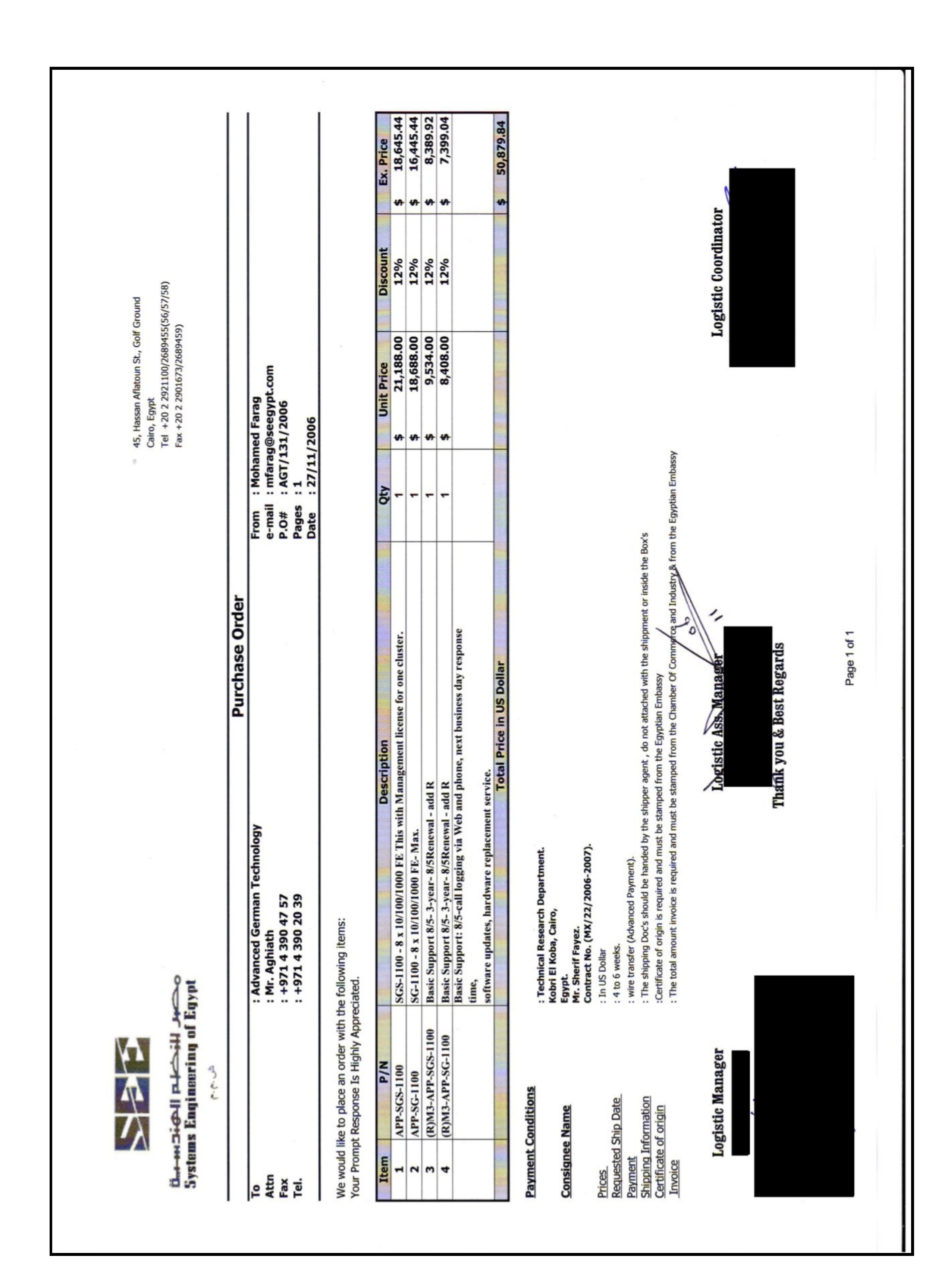
39 *المرجع نفسه.*

40 *المرجع نفسه..*

41 *المرجع نفسه..*

42 *المرجع نفسه.*

ملحق1: أمر شراء من شركة التقنيات الألمانية الحديثة



SEE
مصر للنظم الهندسية
Systems Engineering of Egypt
ش.م.م

45, Hassan Aflatoun St., Golf Ground
Cairo, Egypt
Tel +20 2 2921100/2689455(56/57/58)
Fax +20 2 2901673/2689459)

Purchase Order

To : Advanced German Technology
Attn : Mr. Aghiath
Fax : +971 4 390 47 57
Tel. : +971 4 390 20 39

From : Mohamed Farag
e-mail : mfarag@seegypt.com
P.O# : AGT/131/2006
Pages : 1
Date : 27/11/2006

We would like to place an order with the following items:
Your Prompt Response Is Highly Appreciated.

Item	P/N	Description	Qty	Unit Price	Discount	Ex. Price
1	APP-SGS-1100	SGS-1100 - 8 x 10/100/1000 FE This with Management license for one cluster.	1	$ 21,188.00	12%	$ 18,645.44
2	APP-SG-1100	SG-1100 - 8 x 10/100/1000 FE- Max.	1	$ 18,688.00	12%	$ 16,445.44
3	(R)M3-APP-SGS-1100	Basic Support 8/5- 3-year- 8/5Renewal - add R	1	$ 9,534.00	12%	$ 8,389.92
4	(R)M3-APP-SG-1100	Basic Support 8/5- 3-year- 8/5Renewal - add R	1	$ 8,408.00	12%	$ 7,399.04
		Basic Support: 8/5-call logging via Web and phone, next business day response time, software updates, hardware replacement service.				
		Total Price in US Dollar				$ 50,879.84

Payment Conditions

Consignee Name : **Technical Research Department. Kobri El Koba, Cairo, Egypt. Mr. Sherif Fayez. Contract No. (MX/22/2006-2007).**

Prices : In US Dollar
Requested Ship Date : 4 to 6 weeks.
Payment : wire transfer (Advanced Payment).
Shipping Information : The shipping Doc's should be handed by the shipper agent , do not attached with the shipment or inside the Box's
Certificate of origin :Certificate of origin is required and must be stamped from the Egyptian Embassy
Invoice : The total amount invoice is required and must be stamped from the Chamber Of Commerce and Industry & from the Egyptian Embassy

Logistic Manager [redacted]

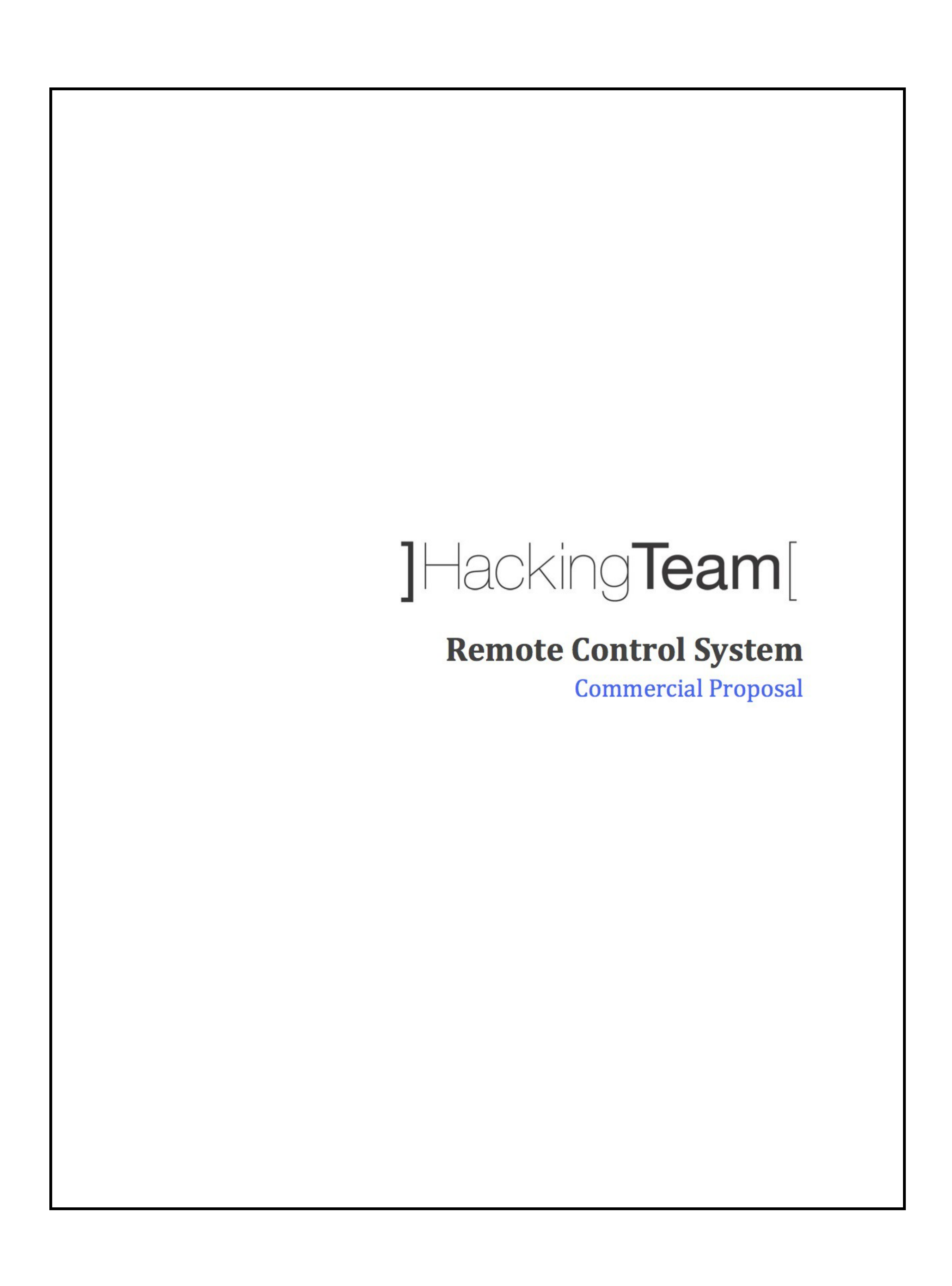
Logistic Ass. Manager [redacted]

Logistic Coordinator [redacted]

Thank you & Best Regards

Page 1 of 1

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية



ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

January 05, 2015

Technical Research Department - TRD
Kobry El Kobba
Cairo - Egypt

Att. Dr. Layla

Offer N. 20140206.009-5.ES

Subject: Proposal for Remote Control System

Dear Sir,

As for your kind request, please find the proposal regarding the Remote Control System – Galileo.

It is however understood that this proposal and the agreement subsequent to your acceptance shall be automatically terminated pursuant to Sections 1353 and ff. of Italian Civil Code should any necessary license or authorization required for the export of the product - under Italian laws, the EU legislation and/or any other applicable laws - be not granted to HT within a period of 120 days from the date of your acceptance. It is also understood that HT shall give notice of the occurrence or the non-occurrence of the Condition in a timely manner, being further agreed that the above condition subsequent can be waived by HT also after its occurrence.

Don't hesitate to contact me for any further information.

Best Regards

[redacted]
Key Account Manager
HT S.r.l.

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Remote Control System Description

Please refer to the following document for technical description:

- HT_Galileo_SolutionDescription_2.3

Remote Control System Technical Requirements

Please refer to the following document for technical requirements:

- HT_Galileo_TechnicalRequirements_v2.3.pdf

Professional Services: Installation and Training

1. **Installation**

The solution will be installed at Customer Site by HT field application engineers.
Duration of the activities is actually planned for one (1) working day and it will be under Customer responsibility to prepare the Operation Environment as indicated in the Technical Requirements document.

2. **Training**

Following the installation, we will provide four (4) days of training focused on the usage of Remote Control System Galileo.
This training will be performed at Client Site.
Please refer to the following document for product training:

- HT_Galileo_Product Training_v1.2

3. **Maintenance & Support**

Maintenance for one (1) year is included.
Please refer to the following document for Maintenance and Support:

- HT_Galileo_SolutionDescription_2.3

4. **On Site Support**

On-site support will be delivered, if requested, by senior Hacking Team Field Application Engineer and will include assistance to the end user in the daily activity.

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Remote Control System Galileo – Quotation Option 1)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	Product Code	Qty
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 13
Platforms		
PC Windows Platform (XP/Vista/7 – 32 & 64bit)	RCS-WIN	Included
Mac-Os Platform	RCS-MAC	Included
Linux Platform	RCS-LIN	Included
BlackBerry Platform	RCS-BB	Included
Android Platform	RCS-AND	Included
iPhone Platform	RCS-IOS	Included
Windows Phone Platform	RCS-WIP	Included
Agents SW License (N. of devices)	RCS-ASL-200	200
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT	EURO	1.000.000,00

(Signature and Stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

REMOTE CONTROL SYSTEM YEARLY SERVICES		
Description	**Product Code**	**Price**
Yearly Attack Vector Service Fee	RCS-EXP	Euro 70.000,00
Yearly Maintenance & Support Service Fee	RCS-MAINT	Euro 132.500,00

REMOTE CONTROL SYSTEM OPTIONAL FEATURES		
Description	**Product Code**	**Price**
Intelligence Module	RCS-INT	Euro 175.000,00

REMOTE CONTROL SYSTEM OPTIONAL SERVICES		
Description	**Product Code**	**Price**
IT- Training (ITTraining_0.4) price per each course up to 5 people	RCS-TRA	Euro 30.000,00
ON-SITE Support Service (8 weeks)	RCS-ONS	Euro 150.000,00

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Remote Control System Galileo – Quotation Option 2)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	**Product Code**	**Qty**
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 5
Platforms		
PC Windows Platform (XP/Vista/7 – 32 & 64bit)	RCS-WIN	Included
BlackBerry Platform	RCS-BB	Included
Android Platform	RCS-AND	Included
Agents SW License (N. of devices)	RCS-ASL-50	50
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT		**EURO 645.000,00**

(Signature and Stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

REMOTE CONTROL SYSTEM YEARLY SERVICES		
Description	Product Code	Price
Yearly Attack Vector Service Fee	RCS-EXP	Euro 70.000,00
Yearly Maintenance & Support Service Fee	RCS-MAINT	Euro 105.000,00

REMOTE CONTROL SYSTEM OPTIONAL FEATURES		
Description	Product Code	Price
Intelligence Module	RCS-INT	Euro 60.000,00

REMOTE CONTROL SYSTEM OPTIONAL SERVICES		
Description	Product Code	Price
IT- Training (ITTraining_0.4) price per each course up to 5 people	RCS-TRA	Euro 30.000,00
ON-SITE Support Service (8 weeks)	RCS-ONS	Euro 150.000,00

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Remote Control System Galileo – Quotation Option 3)

REMOTE CONTROL SYSTEM GALILEO LICENSE		
Description	**Product Code**	**Qty**
Front –End SW License (Collector)	RCS-COL	1
Back- End SW License (Master Node)	RCS-MN	2
Back- End SW License (Shard)	RCS-SH	0
Operators Console		Up to 13
Platforms		
Android Platform	RCS-AND	Included
Agents SW License (N. of devices)	RCS-ASL-50	50
Infection Vectors		
Physical Infection Vectors (USB, CD)	RCS-PHI	Included
Remote Mobile Infection	RCS-RMI	1
Tactical Network Injector	RCS-TNI	1
Yearly Attack Vector Service	RCS-AVS	1 year
Anonymizers SW License	RCS-ANM	3
Alerting Option	RCS-ALM	Included
Remote Control System Installation (1 day)	RCS-INST	(T&A included)
Remote Control System Training (4 days)	RCS-TR	(T&A included)
Remote Control System Advanced Training (5 days in Milan) up to 5 people	RCS-TRM	Included
Yearly Maintenance & Support Service	RCS-MAINT	1 year
TOTAL AMOUNT		**EURO 595.000,00**

____
(Signature and Stamp for Acceptance)

REMOTE CONTROL SYSTEM YEARLY SERVICES

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Description	Product Code	Price
Yearly Attack Vector Service Fee	RCS-EXP	Euro 70.000,00
Yearly Maintenance & Support Service Fee	RCS-MAINT	Euro 95.000,00

REMOTE CONTROL SYSTEM OPTIONAL FEATURES		
Description	Product Code	Price
Intelligence Module	RCS-INT	Euro 60.000,00

REMOTE CONTROL SYSTEM OPTIONAL SERVICES		
Description	Product Code	Price
IT- Training (ITTraining_0.4) price per each course up to 5 people	RCS-TRA	Euro 30.000,00
ON-SITE Support Service (8 weeks)	RCS-ONS	Euro 150.000,00

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Note:

- Every Concurrent Agent license can be used for an unlimited amount of times. Once the investigation is over and the backdoor is uninstalled, it can be used to infect another target.
- The total number of device and platforms can be used in any combination.
- Each agent license will work on any type of operating system that has been bought.
- Hardware Equipment is not included.
- The yearly maintenance fee price is calculated on the purchased configuration, if the configuration changes the maintenance price will be recalculated.
- Remote Attack Vectors Service is a yearly subscription to be purchased every year.
- In refer to the Advanced Training: all travel and accommodations cost are not included
- Prices for additional year of subscription for Maintenance & Support Service and Remote Attack Vectors Service additional are valid for purchase orders received within 2015.

____

(Signature and Stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق2: عرض تجاري مقدم من هاكِنج تِيم إلى إدارة البحوث التقنية

]HackingTeam[

Terms& Conditions

a. Warranty

The warranty period for HT software products is one year starting from date of delivery.

b. Financials

1. Pricing doesn't include VAT and local taxes.
2. Prices are reserved to Technical Research Department - TRD
3. Technical Research Department – TRD accepts to purchase the solution as above reported for a price of Euro
4. The End User Technical Research Department – TRD as to sign the attached "HT_EULAD" and the End User Statement.
5. Software Delivery and Product Training within 45 days upon the Purchase Order is received (to be agreed).
6. Terms of Payment
    - 50% Down Payment at PO date
    - 50% at Delivery Certificate signature date (please refer to the attached document)
7. Validity: The quotation is valid until 30 March 2015

c. List of Attachments:

- HT_Galileo_SolutionDescription_2.3.pdf
- HT_Galileo_Technical Requirements_v2.3.pdf
- HT_Galileo_Product Training_v1.2.pdf
- HT_Galileo_Delivery Certificate_v1.2.pdf
- EULAD
- E.U. Statement_1.0

____
(Signature and stamp for Acceptance)

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

ملحق3: رد من نوكيا



February 22, 2016

Privacy International Report

Nokia is committed to the Universal Declaration of Human Rights and the human rights principles of the United Nations' Global Compact and has embedded them in our Code of Conduct and in our Human Rights Policy. We take steps to ensure that the technology we provide – legally and in good faith – will be used properly and lawfully.

Regarding the case of Egyptian German Telecommunications Industries (EGTI), it was a joint venture of the former Siemens Networks and the Egyptian government, and it transferred to Nokia Siemens Networks with the formation of the joint venture in 2007. Today, Nokia operates in Egypt under Nokia Solutions and Networks S.A.E., a joint venture serving Egyptian telecommunications operators.

As for Universal Advanced Systems, our investigations revealed a commercial arrangement we inherited from Siemens in 2007. We have not pursued new business with Universal Advanced Systems since then.

Regarding Lawful Interception (LI) technology, as a telecommunications equipment vendor we provide LI technology to our operator customers. This capability is a prerequisite for telecommunications operators to obtain a license, and is required by law in virtually all countries globally.

As for monitoring centers, Nokia divested this business in 2009, and we not do we believe that we had any such sales since then. When we sold the business, most customer records were transferred to the new owner and we do not have extensive visibility to possible pre-2009 sales.

Nokia has worked to implement the UN Guiding Principles for Business and Human Rights since they were first launched in 2011. In connection with this work, we were the first telecommunications vendor to define and to implement a human rights due diligence process to minimize and to mitigate the possible risk of misuse of Nokia technology in human rights violations.

As one of the founding members of the Telecommunications Industry Group, we remain committed to constructive dialogue with governments and NGOs around the complex and challenging issues of Internet censorship, privacy and surveillance.

Should you have any further questions, please do not hesitate to contact us at any time.

Sincerely yours,

Sandra Cornet-Vernet Lehongre
Director, Corporate Responsibility

ملحق4: رد من هاكِنج تِيم

Dear Ms. Blum-Dumontet:

As you know, Hacking Team software is sold exclusively to governments and government agencies. Sales are regulated by Italian authorities. In cases in which a separate company is involved, Hacking Team still requires end users to certify in their contracts that the software will be used for lawful purposes and not used for any military activity. However, as you also know, the company does not identify individual clients or confirm information gleaned from stolen documents.

Privacy International has been a relentless critic of Hacking Team, and has enjoyed a good deal of publicity from this criticism. Nonetheless, I hope you will permit me to make a couple of obvious but generally ignored points about the product this company has developed and sells.

Of course, safeguards are important. That is why Hacking Team complies voluntarily and fully with the Wassenaar protocols implemented in Italy more than a year ago. For a Hacking Team sale to take place - to Egypt or elsewhere - it must be approved by the Italian authorities. We believe we are the only supplier of legal surveillance software to be subject to such regulation. Beyond complying with regulation, Hacking Team has always required customers to certify that they will use Hacking Team technology legally and not for military purposes. In fact, despite all the evidence published after the illegal attack on the company last July, there is nothing to show the company acted in any way illegally or in violation of any ban or regulation. Furthermore, the evidence clearly snows this technology is used as intended for law enforcement investigation and that the use of the technology is limited.

It is also worth noting that the sale of legal surveillance technology to Egypt is entirely legal. Egypt is an ally of the West including the U.S, most European countries and even of Israel. Not only is the sale of software to Egypt permitted, but also Western governments permit the sale of heavy weapons including F-16 fighter planes and Harpoon missiles to Egypt.

Finally, the sale of software for lawful surveillance is important for the protection of all of us. That is not only true of sales of such software to Western countries. Indeed, it may be even more important to provide tools for investigations in countries where there is wide-spread crime or terrorism or both. It should be obvious that investigating terrorists and their organizations in such a country could lead to the prevention of an attack in Paris, London or Berlin by those trained, financed and supported by elements that are active in the Middle East and elsewhere.

I hope you will include a full perspective of the situation in your forthcoming report.

Eric

ملحق5: رد من سيمنس

Dear Mrs. Blum-Dumontet,

Thank you for your inquiry. First, I would like to make you aware that Siemens has transferred its network business to Nokia Siemens Networks, in April 2007. All relevant documents have been transferred to Nokia Siemens Networks as well, so we are not able to comment on the business that is related to Nokia Siemens Networks. Nokia Siemens Networks had been consolidated by Nokia.

In August 2013, Nokia Siemens Networks became Nokia Solutions and Networks. It is since then wholly owned by Nokia and will continue to be consolidated by Nokia.

I would like to ask you to address your questions to Nokia as we are unable to verify and to comment on your research.

Best regards,
Wolfram Trost